

(TS//SI//REL)VPN SigDev Basics



S31244 - OTTERCREEK

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20341101

Overall Classification:

TOP SECRET//COMINT//REL TO USA, FVEY

(U) What is a VPN?

- (U) A Virtual Private Network or VPN is a computer network that uses encryption to securely connect remote users/networks over an otherwise insecure network, usually the public internet.
- (U) Common Types:
 - PPTP, IPsec, SSL
- (U) Public Key Encryption
 - Diffie-Hellman, RSA

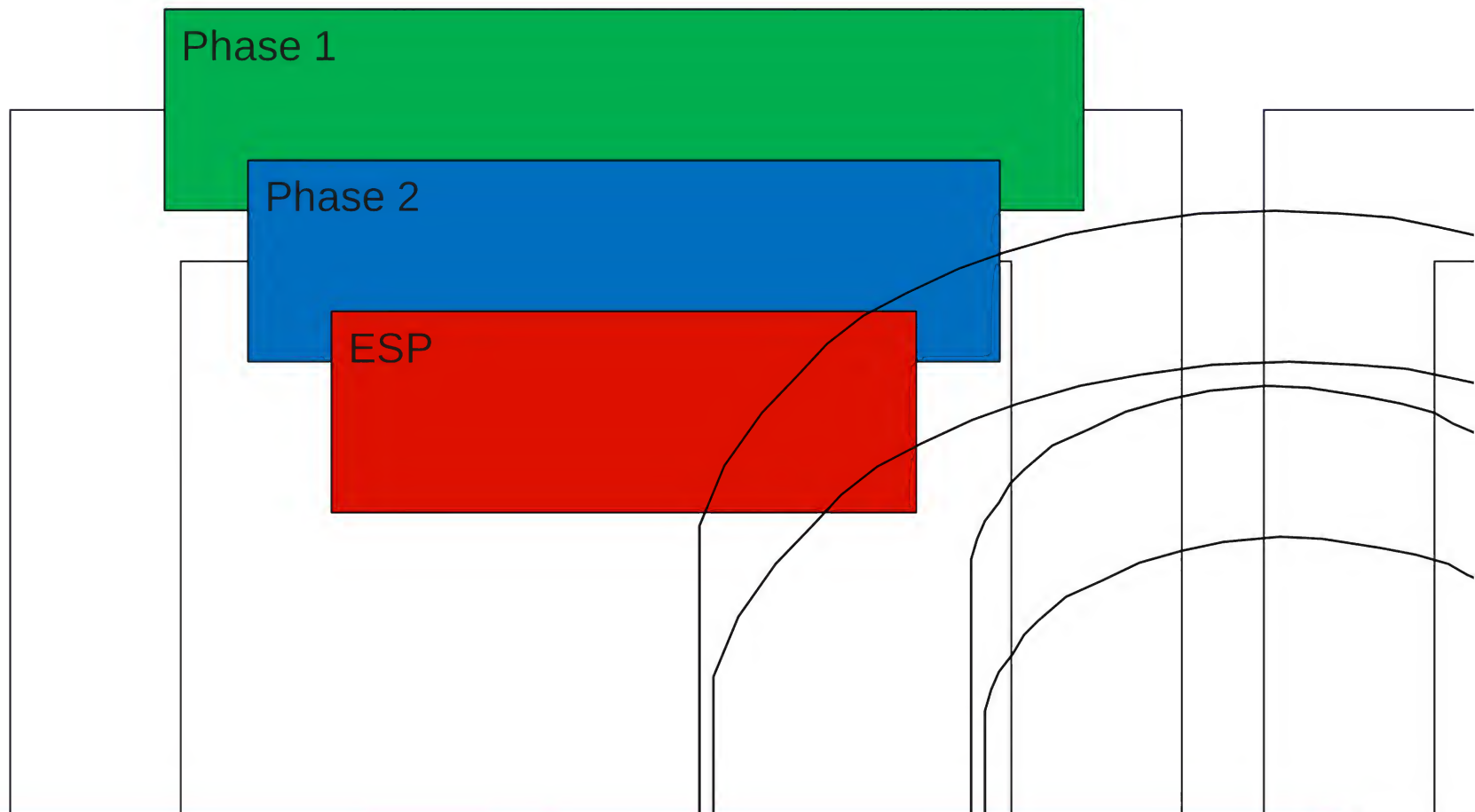
(U) PPTP

- (U) Microsoft Point-to-Point Tunneling Protocol
- (U) Control Channel
 - TCP port 1723
- (U) Data Channel
 - GRE-Next Protocol 47
- (U) RFC 2637, RFC 3078

(U) IPSec

- (U) Authentication
 - Pre-shared key (PSK) or Public key certificates
- (U) ISAKMP/IKE packets are used for key exchange and to establish the secure connection
 - UDP port 500, 4500; TCP port 500
- (U) ESP packets contain the encrypted data
 - IP Next Protocol 50; UDP port 500
- (U) RFC2402, RFC2406, RFC2409, RFC4306, RFC2408

(U) IPSec in a nutshell



(U) SSL/TLS

- (U) Secure Sockets Layer/Transport Layer Security
- (U) WARNING! e-commerce = tons of uninteresting SSL traffic
- (U) Common ports: TCP ports 443, 995
- (U) RFC2246, RFC4346, RFC5246

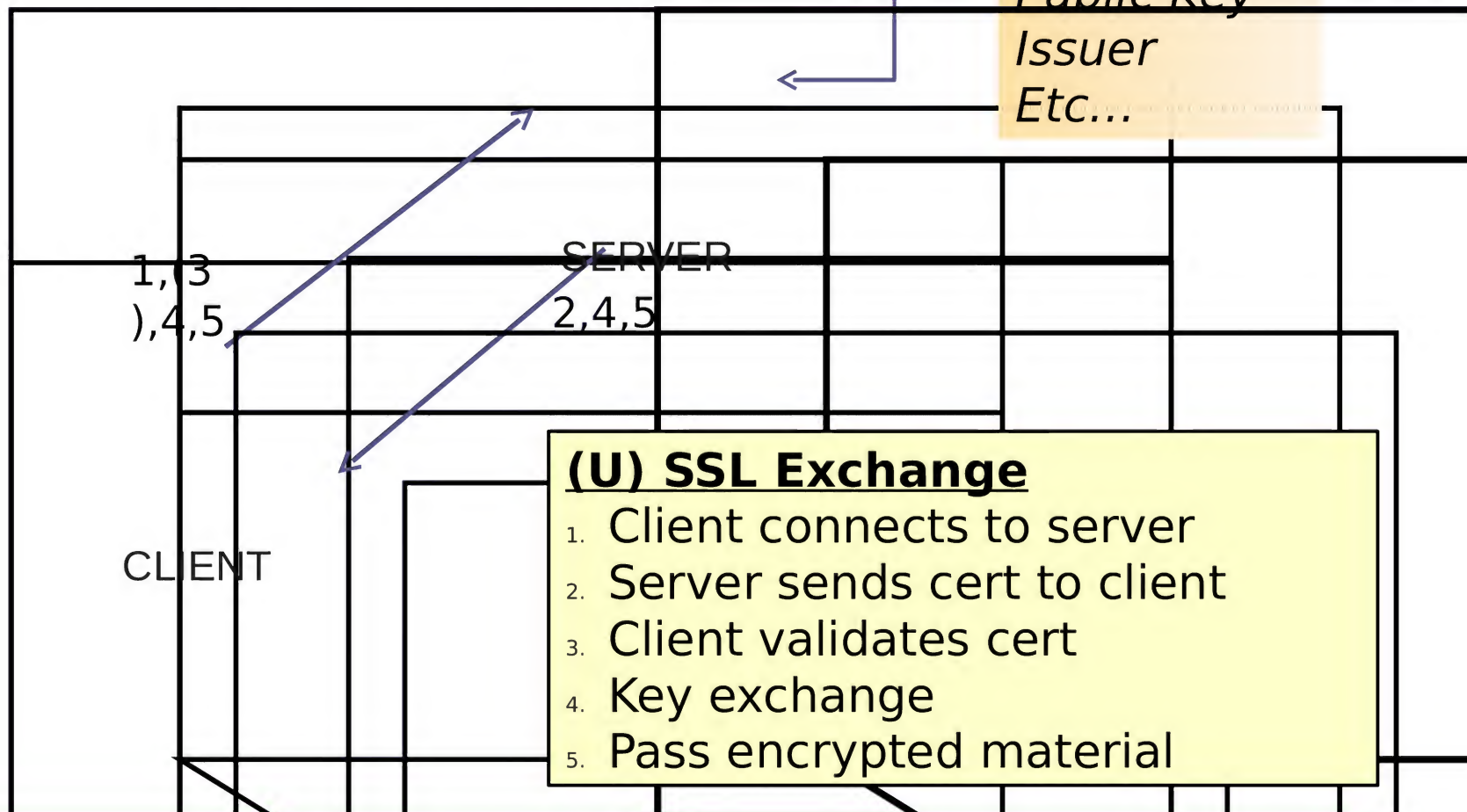
□



(U) SSL in a nutshell

Certificate

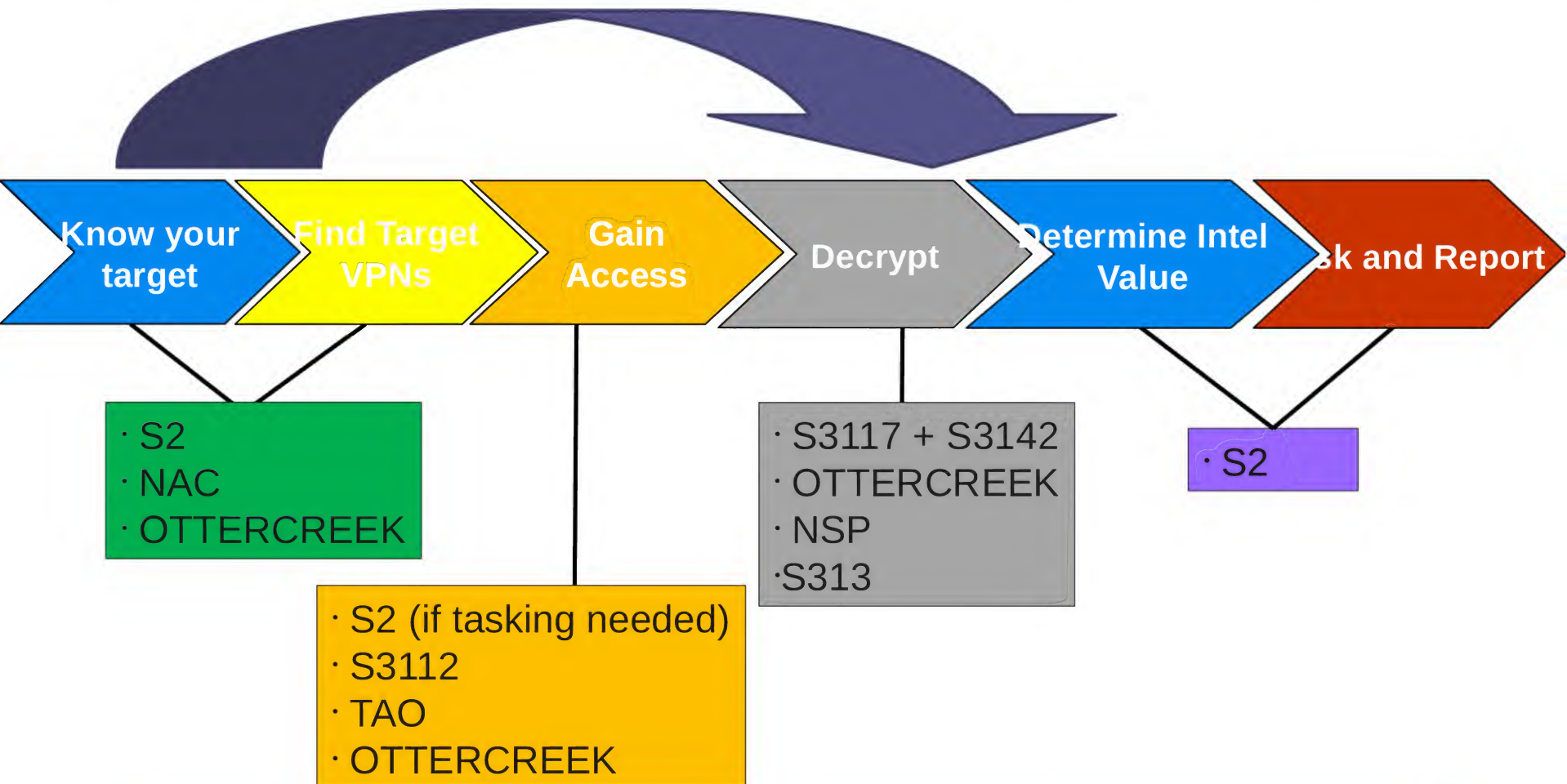
*Subject
Validity
Public Key
Issuer
Etc...*



(TS//SI/REL) Who works VPNs?

- (TS//SI//REL) VPN Working Group (go vpn)
[REDACTED]
 - S2, SSG, CES (OTTERCREEK, NSP, S31322, S3117, S3112), TAO, etc.
- (TS//SI//REL) Alias: [REDACTED]
(Board alias: [REDACTED])
- (TS//SI//REL) Meets every other Thursday at 1300

(TS//SI/REL) Who works VPNs?



(TS//SI//REL) So you think your target is using a VPN...

(TS//SI//REL) SigDev Tools

(TS//REL) VPN Specific

- ~~BLEAKINQUIRY~~
- **DISCOROUTE**
- **TOYGRIPPE**

(TS//REL) Also useful

- MARINA
- MASTERSHAKE
- NKB
- PINWALE
- RENOIR
- TREASUREMAP
- TUNINGFORK
- **XKEYSCORE**

(TS//SI//REL) TOYGRIPPE

- (TS//SI//REL) Database of VPN metadata
 - IPSec, PPTP, ViPNet

Click to edit Master text styles

Second level

Third level

Fourth level

Fifth level

(TS//REL) **TYG Tips:**

- Populate "Display Fields"
- For both directions between 2 Ips, use **AND**
- For either direction connecting to a single IP, put IP in both "Source" and "Destination" boxes, and use **OR**

Standard Form - Mozilla Firefox

File Edit View History Bookmarks Tools Help

XKEYSCORE OYGRIPPE NKB: Home NKB Disco Route Roadred.net MyPage GoldPoint

XK Results

Logoff

Query

Standard

FreeForm

Results

AllResults

View

Excel

Text

Delimited

Preferences

General

Help

FAQ

Contact Us

Execute Clear All

Date Range(Required):

START: 4 / 1 / 2011 00 : 00

END: 4 / 5 / 2011 00 : 00

Data Fields:

** Use checkboxes to exclude the indicated value. **

Sites ***** Add

☐ Selected Sites Remove

Sources ACTIVE_SURVEY Add

☐ Selected Sources Remove

☐ Case Notation

☐ Vendor Name

☐ Source CIDR

☐ Destination CIDR

☐ Source Company

☐ Dest. Company

☐ Source Country

☐ Dest. Country

☐ Source Domain

☐ Dest. Domain

☐ Info Name

Query data fields based on AND constraints.

Save Standard Query:

Query Name:

Description:

Store

Execute Clear All

Display Fields:

Timestamp

Add Remove

Field Information:

* Timestamp: The timestamp of the traffic as provided by the source. (dtTime, timestamp)

Timestamp

Case Notation

Site

VPN Type

Geo Source Country

Source IP Address

Destination IP Address

Geo Destination Country

IPSEC Authentication Name

Sort Up Down

Save as default Clear Reset to Default

IP Addresses(Ranges and Wildcards Accepted):

Source IP Addresses

Destination IP Addresses

Source IP Ports

Destination IP Ports

Clear Addresses File...

Clear Addresses File...

Constrain results to source AND destination IP Address matches

Query Results - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Click to edit Master text styles

XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Results

Query Results

TS//SI//REL TO USA, FVEY	2011-04-02 08:29:38.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-02 09:13:14.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-02 10:48:10.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-02 11:31:53.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 12:22:03.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 11:08:00.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 11:54:35.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 13:24:56.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 14:58:08.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-01 11:37:49.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-01 17:37:33.0	KLV125899750000	US-966E	ESP	DE	IR	
TS//SI//REL TO USA, FVEY	2011-04-01 12:51:08.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-01 00:08:15.0	IRS1037	DS-300	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-01 00:23:25.0	IRS1037	DS-300	IKEv1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-03 05:41:27.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 06:25:53.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 07:56:09.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 08:42:05.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 09:32:55.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 10:16:16.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 10:59:38.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 11:50:29.0	IR1S035	DS-200B	IKEv1	DE	IR	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 12:34:43.0	IR1S035	DS-200B	IKEv1	DE	IR	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 12:34:45.0	IR1S035	DS-200B	IKEv1	DE	IR	
TS//SI//REL TO USA, FVEY	2011-04-03 12:34:44.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 11:23:51.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 13:23:50.0	IR1S035	DS-200B	IKEv1	DE	IR	pre-shared key
TS//SI//REL TO USA, FVEY	2011-04-03 13:23:51.0	IR1S035	DS-200B	IKEv1	DE	IR	
TS//SI//REL TO USA, FVEY	2011-04-02 06:52:02.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 05:07:51.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 06:16:31.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 07:48:23.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 05:34:51.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:18:42.0	KLDAB00001M1100	UKJ-260D	IKEv1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:01:51.0	KLDAB00001M1100	UKJ-260D	ESP	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:18:41.0	IRS1037	DS-300	IKEv1	IR	DE	
TS//SI//REL TO USA, FVEY	2011-04-02 00:16:51.0	IRS1037	DS-300	ESP	IR	DE	

Done

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Second level

Third level

Fourth level

Fifth level

ø (U) Export results to excel or text doc for easier sorting.

(TS//SI//REL) XKEYSCORE

(TS//REL) Fingerprints

- IPSec
 - vpn/esp
 - vpn/isakmp
- PPTP
 - vpn/pptp*
- SSL
 - network_encryption/ssl

(TS//REL) Search Forms

- Start with **FULL DNI**
 - **vpn/***
 - **network_encryption/***
- IPSec
 - IKE Parser
- SSL
 - SSL Parser

Firefox browser window titled "XK Search: Full Log - Mozilla Firefox". The address bar shows "ic.gov". The page header includes "XKEYSCORE" and a warning: "Warning: your password has expired!". The main content area is titled "Search: Full Log" and displays a search form with the following fields:

- Query Name: [Redacted]
- Justification: ("S//SI//REL) Looking for IPsec traffic to perform vulnerability assessment. [Recent Justifications](#)
- Additional Justification: [Dropdown]
- Miranda Number: [Text]
- Current Time: 2011-04-04 14:04:04 GMT
- Datetime: 1 Day, Start: 2011-04-03 00:00, Stop: 2011-04-05 00:00
- Client IP (X-Fowardec-For): [Text] [\[P Address Field Builder\]](#)
- DVBS MAC: [Text]
- DVBS PID: [Text]
- WLAN Channel: [Text]
- WLAN SSID: [Text]
- WLAN BSSID: [Text]
- WLAN DMAC: [Text]
- WLAN SMAC: [Text]
- S GAD: [Dropdown]
- 3PRSTLLI: [Text]
- Active User/realms: [Text]
- IP Address: [Text] [\[Address Field Builder\]](#)
- IP Address: [Text] [\[Address Field Builder\]](#)

The bottom of the page features a red circle highlighting the two IP Address fields. The footer contains the text "Done" and a copyright notice: "This system is built for US/EU/18 and Human Rights Act compliance".

XK Search: Full Log - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov

XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Search Full Log Standard Form

This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//NOFORN

XKEYSCORE Welcome srwts2! [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum

Navigation Filter

Search Wizard

- CNE
- Classic
 - MultiSearch
 - Classic A-M
 - Alert
 - BlackBerry
 - Call Logs
 - Category DNI
 - Cellular DNI
 - Cisco Passwords
 - Clarent
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Geo Info
 - HTTP Activity
 - IKE Parser
 - Keylogger
 - Logins and Password
 - Machine Info
 - Microplugin Metadata
 - Obfuscation (Munged)
 - Classic V-Z
 - Network Information
 - Network Logs
 - PILBEAM
 - PDF VoIP Metadata
 - Passports from Images
 - Phone Number Extract
 - RBGAN
 - RTP
 - Radius Logs
 - Registry
 - SIP
 - SSH Parser
 - SSL Parser
 - Shellcode
 - TDI
 - TIPOFF Collection
 - Topic / Tech Strings
 - User Activity
 - User Activity (NewExp)

Port: From To

Country: ILS AND IGB AND ICA AND INZ AND IAU From To One side is not 5-eyes

Country: ILS AND IGB AND ICA AND INZ AND IAU To Both sides are not 5-eyes

City (IP): From To

Latitude (IP): From To

Longitude (IP): From To

Map Field Builder regions (IP): [Map Field Builder](#)

Outer Tunnel IP Address: From To [IP Address Field Builder](#)

Outer Tunnel IP Address: To [IP Address Field Builder](#)

Outer Tunnel Port: From To

Outer Tunnel Port: To

Application Type*:

Application Info*:

Application: vpn*

ApplID (+Fingerprints)* [Fulltext](#) [Populate with Field Builder](#) [Populate with Tree Field Builder](#)

Case/operation:

This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//NOFORN

Done

Ø (TS//REL) For initial searches, you may want to leave this blank to see all of the different kinds of traffic are found on the IP pair.

XK Metaviewer: [redacted] vpn - Mozilla Firefox

File Edit View History Bookmarks Tools Help

lc.gov

XKEYSCORE TOYGRIPPE NKB Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Metaviewer: 84.11.25.13... x Standard Form x NKB Disco Route x https://ncmd...248823681254 x

This system is audited for USSID18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome swits2! [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum

Navigation Filter [redacted] vpn

Search Wizard

- CNE
- Classic
 - MultiSearch
 - Classic A-M
 - Alert
 - BlackBerry
 - Call Logs
 - Category DNI
 - Cellular DNI
 - Cisco Passwords
 - Clarent
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Geo Info
 - HTTP Activity
 - IKE Parser
 - Keylogger
 - Logins and Passwords
 - Machine Info
 - Microplugin Metadata
 - Obfuscation(Munged T
 - Classic N-Z
 - Network Information
 - Network Logs
 - PILBEAM
 - PPF VoIP Metadata
 - Passports from Images
 - Phone Number Extract
 - RBGAN
 - RTP
 - Radius Logs
 - Registry
 - SIP
 - SSH Parser
 - SSL Parser
 - Shellcode
 - TDI
 - TIPOFF Collection
 - Topic / Tech Strings
 - User Activity
 - User Activity (NewExp

Help Actions Reports View Map View

Sigad	Casnotation	Datetime	Datetime E	Fm Port	Fm City (IP)	Fm Co Fm IP	To IP	To Cou	To City (IP)	To Port	Application	AppID (+Fingerprints)
UKJ-260D	KLDAB00001M1100	2011-04-03 00:00:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:03:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:06:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:09:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:12:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:15:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:18:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:21:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:22:01	2011-04-03 500							500	vpnl/lsakmp	vpnl/lsakmp vpnl/lsac/lsakmp/main_mode/key_exchange_message vpnl/ire_4 vpnl/lsakmp_content
UKJ-260D	KLDAB00001M1100	2011-04-03 00:24:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:27:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:30:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:33:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:36:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:39:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:42:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:45:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:51:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:54:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 00:57:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:00:52	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:06:31	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:07:58	2011-04-03 500							500	vpnl/lsakmp	vpnl/lsakmp vpnl/lsac/lsakmp/main_mode/key_exchange_message vpnl/ire_4 vpnl/lsakmp_content
UKJ-260D	KLDAB00001M1100	2011-04-03 01:09:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:12:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:15:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:18:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:21:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:24:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:30:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:33:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:36:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:39:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:42:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp
UKJ-260D	KLDAB00001M1100	2011-04-03 01:45:53	2011-04-03 0							0	vpnl/esp	vpnl/esp nac/vpn/protocols/esp

Page 1 of 24 Page Size 50 (Max 100 rows per page)

Displaying 1 - 50 of 1171

jb_S8F22_00978567001301926190_1

This system is audited for USSID18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Done

XK Metaviewer: CREAKSTILE_HW_PK - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov

XKEYSCORE TOYGRIPPE NKB: Home NKB Disc Route Roadbed.net MyPage GoldPoint

XK Results XK Metaviewer: CREAKSTILE... Query Results

This system is audited for USSID 19 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome snwils2! [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum

Navigation Filter

Search Wizard

CNE

Classic

MultiSearch

Classic A.M

Alert

BlackBerry

Call Logs

Category DNI

Cellular DNI

Cisco Passwords

Client

DNS

Document Metadata

Document Tagging

Email Addresses

Extracted Files

Full Log DNI

Geo Info

HTTP Activity

IKE Parser

Keylogger

Logins and Passwords

Machine Info

Microplugin Metadata

Obfuscation (Munged)

Classic N.Z

Network Information

Network Logs

PILBCAM

PPF VoIP Metadata

Passports from Images

Phone Number Extract

RBCAN

RTP

Radius Logs

Registry

SIP

SSH Parser

SSL Parser

Shellcode

TDI

TIPOFF Collection

Topic / Tech Strings

User Activity

User Activity (NewExp)

Histogram Grid

Page 1 of 1

Filter: Fm IP To IP Count

132

72

46

38

CREAKSTILE_HW_PK

Help Act ons Reports View Map View FILTERS: [X]

	State	ID	Classification	Sigad	Casensation	Datetime	Fm Port	Fm City (IP)	Fm Co	Fm IP	To IP	To Cou	To City (IP)	To Port	Application	AppID (+Fingerprints)
1		226	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content vpn/isakmp.ph
2		263	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp phase1_policy
3		264	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp phase1_policy
4		294	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:41:04	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content vpn/isakmp.ph
5		261	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:46:33	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
6		262	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:46:33	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
7		269	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:49:00	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
8		260	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 00:49:00	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
9		265	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 01:45:31	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
10		266	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 01:45:31	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
11		267	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 02:42:40	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
12		268	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 02:42:40	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
13		162	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE087A000HDO	2011-04-01 03:27:09	500							500	vpn/isakmp	vpn/isakmp vpn/device/ipsec vpn/isakmp phase
14		237	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE087A000HDO	2011-04-01 03:27:09	500							500	vpn/isakmp	vpn/isakmp vpn/device/ipsec vpn/isakmp phase
15		271	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE087A000HDO	2011-04-01 03:34:12	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content vpn/isakmp.ph
16		272	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE087A000HDO	2011-04-01 03:27:10	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content vpn/isakmp.ph
17		163	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 03:34:12	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
18		236	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 03:34:12	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
19		1	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE087A000HDO	2011-04-01 03:58:52	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
20		2	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE087A000HDO	2011-04-01 03:58:52	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
21		10	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 07:15:29	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
22		247	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 07:15:29	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
23		175	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 08:24:36	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
24		230	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 08:24:36	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content
25		3	TOP SECRET//COMINT//REL TO USA, AUS, CAN, I	UKC-302A	PKCSE018A000HDO	2011-04-01 08:24:38	500							500	vpn/isakmp	vpn/isakmp vpn/isakmp content

Page 1 of 6 Page Size: 50 (Max 100 rows per page)

Displaying 1 - 50 of 298

jb_58f22_00966248001301946356_1

This system is audited for USSID 19 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

https://bks-central.com/psa/ic.gov/8443/XKEYSCORE/metaviewer/metadata/list.do?nuarId=jb_58f22_00966248001301946356_1#

(TS//SI//REL) PINWALE

- (TS//SI//REL) Both VPN traffic and Sys Admins passing information about VPN setup
- (TS//SI//REL) IP addresses and port numbers (ex. AP 00500) *****Document Zone = C2C**
- (TS//SI//REL) Display 'DZ Protocol SRC Port', 'DZ Protocol DEST Port', 'Next Protocol Name'

(TS//SI//REL) DISCOROUTE

- (TS//SI//REL) Router configuration data
 - From passive and active collection
 - Key terms to search for within configs:
 - 'crypto map', 'isakmp', 'ipsec', 'pre-shared-key'

NKB Disco Route - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov

XKEYSCORE TOYCRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Results Query Results NKB Disco Route TREASUREMAP - TOOLS

Network Knowledge Base DiscoRoute (Version 2.14) NKB HOME

Combined Query Network Mgmt Query (Coming Soon) Help Feedback

DiscoRoute Combined Query

Submit CSV Tips: If TAO has a Point of presence, you will see it manifest tag in results. Query History:

☐ Collapse Results by hostname/sigad

General Query Terms

Text Query

Date

Start Date: End Date:

☐ DOI ☐ Load Date ☒ Entire Database

Vendor

☒ Cisco ☒ Huawei ☒ Infinet
☒ Juniper ☒ Mikrotik ☒ Tenorswitch

Select All Clear All

IP Address

IP Address: (1.2.3.4 or 1.2.3.4[CIDR] or 1.2.3.4 - 3.4.5.4)

IP Range Search

☒ Interfaces - Subnet
☒ Static Route IP
☒ Access Lists
☒ Routing Protocol IP

Exact IP Search

☒ IP Header FROM/TO
☐ Interfaces - Export
☒ Anywhere else in the XML

Limit Search to CIDR Ranges Smaller Than (or equal to): /24

Select All Clear All Any checked items can be found (OR condition) in config

Manifest (Cisco Only)

☐ A - EQUANT ☐ I - Show Interfaces ☐ P - Voip
☐ B - BGP ☐ K - Crypto Keys ☐ R - Show Run
☐ D - Show CDP ☐ M - Multihop ☐ T - Tacacs
☐ G - GPRS ☐ N - Tgt Net Service ☐ V - Show Version
☐ H - TAO Pop ☐ O - OSPF

Clear All All checked items must be found (AND condition) in config

Session ID:

Clear Panel

Hostname: SIGAD: Case: Country: TAO Project Name: AS Number: AS: Seen in Config Derived Snmp Community: IOS Image Name: Device Type:

Done

NKB Disco Route - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google

XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint

XK Results Standard Form NKB Disco Route https://ncmd...255963345563 https://ncmd...256303960492 https://ncmd...299304204961

Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON//NOFORN//20320108

Network Knowledge Base DiscoRoute (Version 2.14) NKB HOME

Combined Query Network Mgmt Query (Coming Soon) Help Feedback

Detailed Combined Command Results

Hostname	Model	DOI	Vendor	Sigad	Case	Manifest	IOS Image	Source IP	S Country	S City	Session	Qualit	SPort	DPort	E
GW_SMS		2009-12-29	huawei	USD-1031TE	MINDAQ						4432	18	00023	12488	
GW_SMS		2009-12-15	huawei	USD-1031TE	MINDAQ						25956	20	00023	13320	
GW_SMS		2009-12-15	huawei	USD-1031TE	MINDAQ						25956	20	00023	13320	
		2009-11-13	cisco	USD-1031TE	MINDAQ						96	9	00023	13429	
A6-VPN		2009-10-22	huawei	USF-790	SCDVB0000001MWC	R					23965	51	00023	01327	
A6-VPN		2009-10-22	huawei	USF-790	SCDVB0000001MWC	R					17894	55	00023	01327	
A6-VPN		2009-10-13	huawei	USF-790	SCDVB0000001MWC	R					8809	47	00023	01089	
		2009-10-02	huawei	USD-1031TE	MINDAQ						57299	1	23	13332	
		2009-09-10	huawei	USD-1031TE	MINDAQ						4210	1	23	15073	
		2009-09-10	huawei	USD-1031TE	MINDAQ						4905	1	23	13841	
		2009-06-15	huawei	USF-790	SCDVB0000001MWC						31407	54	23	1031	

Page 1 of 1 Save as CSV Save Files to Disk Compare Results Summary Mailorder Out Map in Render View Related Find Related Results 1 - 33

Payload XML Summary Map Query Parameters Open in New Window

```
password cipher JS, [51EA, '4B, \#C3YB91!!
service-type telnet terminal
level 3...I...L
#
ike proposal 10
encryption-algorithm 3des-cbc
dh group21..U..
#
ike peer peer_hq
exchange-mode aggressive
pre-shared-key Key4Cuba-A6
id-type name
remote-address [REDACTED]
nat traversal
peer multi-subnet.I.v..
ipsec proposal proposal_ph2
esp authentication-algorithm sha1
```

Powered by the SIGDEV Lab
Version Number: 2.14 New
Last Modified Date: March 14, 2011
Last Reviewed Date: March 14, 2011
Content Steward: [REDACTED] SSG21, 969-3341
Page Publisher: [REDACTED] CON, SSG21, 969-0342

NAC

Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON//NOFORN//20320108

Find: [REDACTED] Match case

Done

NKB Disco Route - Mozilla Firefox

File Edit View History Bookmarks Tools Help

IC.gov Google

XKEYSCORE TOYGRIPPE NKB Home NKE Disco Route Roadbed.net MyPage Go dPoint

XK Results Standard Form NKB Disco Route https://rcmd...248823681254

Dynamic Page -- Highest Possible Classification is TOP SECRET//COMINT//ORCON//NOFORN//20320106

Network Knowledge Base DiscoRoute (Version 2.14) NKB HOME

Combined Query Network Mgmt Query (Coming Soon) Help Feedback

DiscoRoute Combined Query

Submit CSV Tips: This is the new DISCOROUTE webserver. Update any bookmarks to bring you here. Query History:

☐ Collapse Results by Hostname/Sigad

General Query Terms

Text Query UNAMI

Date

Start Date End Date

☐ DOI ☐ Load Date ☒ Entire Database

Vendor

☒ Cisco ☒ Huawei ☒ Infinet
☒ Juniper ☒ Mikrotik ☒ Tenorswitch

Select All Clear All

IP Address

IP Address: (1.2.3.4 or 1.2.3.4/24 or 1.2.3.4 - 3.4.5.6)

IP Range Search
☐ Interfaces - Subnet
☐ Static Route IP
☐ Access Lists
☐ Routing Protocol IP

Exact IP Search
☐ IP Header FROM/TO
☐ Interfaces - Exact
☐ Anywhere else in the XML

Limit Search to CIDR Ranges Smaller Than (or equal to):

Select All Clear All Any checked items can be found (OR condition) in config

Manifest (Cisco Only)

☐ A - EQUANT ☐ I - Show Interfaces ☐ P - Voip
☐ B - 3GP ☒ K - Crypto Keys ☐ R - Show Run
☐ D - Show CDP ☐ M - Multihop ☐ T - Tacacs
☐ G - GPRS ☐ N - Tgt Nat Service ☐ V - Show Version
☐ H - TAC Pop ☐ O - OSPF

Clear All All checked items must be found (AND condition) in config

Session ID:

Clear Panel

Hostname: SIGAD: Case: Country: TAO Project Name: AS Number: AS: Seen in Config Derived: Snmp Community: IOS Image Name:

Combined Query Network Maint Query (Coming Soon) Help Feedback

Detailed Combined Command Results

Hostname	Model	DOI	Vendor	Sigad	Case	Manifest	IOS Image	Source IP	S Country	S City	Session	Qualit	S Port	D Port	E
VPN01-UNAMI-E		2009-06-09T	cisco	UKC-125W	G2B7000001MWC	D_K_PR				RESERVED	109460	78	23	61470	
GILAT-HR15926	c2600	2009-10-15T	cisco	UKC-125W	G2B8200001MWC	D_K_RT	c2600-advs			RESERVED	134422	75	00023	00319	
GILAT-HR15926	c2600	2009-10-31T	cisco	UKC-125W	G2B8200001MWC	D_K_R	c2600-advs			RESERVED	38202	75	00023	02012	
kuw-hub		2009-10-15T	cisco	UKC-125W	G2B6900001MWC	D_K_R				RESERVED	32879	74	00023	50554	
kuw-hub		2009-10-15T	cisco	UKC-125W	G2B6900001MWC	D_K_R				RESERVED	32879	74	00023	50554	
kuw-hub		2009-10-15T	cisco	UKC-125W	G2B7900001MWC	D_K_R				RESERVED	30000	74	00023	50554	
VPN02-UNAMI-K		2009-09-10T	cisco	UKC-125W	G2B8200001MWC	D_K_PR	c2800nm-ad			RESERVED	59890	73	23	3408	
r-unami-kuw-isp		2009-01-16T	cisco	UKC-125W	G2B6900001MWC	D_K_R				RESERVED	26342	71	23	59226	
ISPO2-UNAMI-AH		2009-07-03T	cisco	US-967J	1AH116337454200	B_K_OPR				DUBAI	29872	71	23	27714	
bdr01-unami-kir		2009-06-07T	cisco	UKC-125W	G2B7000001MWC	D_K_PR				DUBAI	23927	69	23	64278	
bdr01-unami-kir	c2800nm	2010-06-22T	cisco	UKC-125W	G2B67000001MWC	D_K_PR	c2800nm-ad			RESERVED	40264	68	00023	44003	

Page 1 of 2 Save as CSV Save Files to Disk Compare Results Summary Mailorder Out Map in Renoir Find Related Results 1-200 c

[Payload](#)
[XML](#)
[Summary](#)
[Map](#)
[Query Parameters](#)
[Open in New Window](#)

```
*
*                                     UNAMI
*
*                               Authorized Personnel Only
*
* If you do not have explicit authorization issued by UNAMI NMU to access
*       this H
*
C device, leave now!                                *
*
* System: [REDACTED]
* IP Add: [REDACTED]
*
* DESCRIPTION : THIS ROUTER IS THEVOICE GATEWAY INTENDED FOR USE WITH THE H
g( * [REDACTED]
*
* FEATURES
*
*   1. NO IS EVER CONNECTED TO LOCAL LAN
```

NAC **Powered by the SIGDEV Lab**
Version Number: 2.14 **Here!**
Last Modified Date: March 14, 2011
Last Reviewed Date: March 14, 2011
Content Steward: [REDACTED]
Page Publisher: [REDACTED]

Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON//NOFORN//20320108

(U) Others

- (TS//REL) NKB
- (TS//REL) TUNINGFORK
- (TS//REL) TREASUREMAP
- (TS//REL) RENOIR
- (TS//REL) MASTERSHAKE
- (TS//REL) ROADBED
- (TS//REL) ~~BLEAKINQUIRY~~

(TS//SI//REL) Basic VPN rules of thumb

(TS//REL) If you have an IP address...

- Check TOYGRIPPE and XKS
 - Look for paired traffic
- For IPsec, check sys admin chatter for PSK (DISCOROUTE; PINWALE; MARINA)
- Share your data with OTTERCREEK for vulnerability assessment (XKEYSCORE or DROPBOX)
- Submit tasking

(TS//REL) If you don't ...

- Look in DISCOROUTE
- Query Sys Admins in PINWALE and MARINA
- Check your targets TAO projects

EITHER WAY,
JOIN THE
VPN WORKING GROUP
FOR ALL OF YOUR
VPN SIGDEV NEEDS

(U//FOUO) Useful Links

- (TS//SI//REL) VPN Working Group (go vpn) [REDACTED]
- (TS//SI//REL) OTTERCREEK (go VPN XFT)
[REDACTED]
 - VPNXFT DROPBOX[REDACTED]
- (TS//SI//REL) Network Security Products (go NSP)
[REDACTED]

(U) Questions?

[REDACTED]

[REDACTED]

OTTERCREEK

[REDACTED]